curso livre

Estácio

FUNDAMENTOS DE *BLOCKCHAIN* E OPORTUNIDADES RELACIONADAS ÀS CRIPTOMOEDAS

SUMÁRIO

FUNDAMENTOS E APLICAÇÕES DA TECNOLOGIA *BLOCKCHAIN*

Blockchain (ou cadeia de blocos) é uma tecnologia de troca de informações e armazenamento de dados de forma distribuída, segura e barata que usa recursos como criptografia assimétrica e assinatura digital para garantir segurança nas transações/operações. É vista como uma "bala de prata" para viabilizar transações eletrônicas que exijam confiabilidade sem a necessidade da existência de um intermediário entre as partes para atestar a validade da transação/operação. *Blockchain* viabiliza transações P2P (Peer-to-Peer, ou pessoa com pessoa) confiáveis sem autoridade de intermediação. Se implementada em situações de uso cotidiano, pode eliminar a necessidade de imobiliárias, cartórios, bancos centrais, órgãos de controle etc.

Saiba mais

Entenda nesse vídeo o que é, como funciona e onde se utiliza a *blockchain*: <*https://youtu.be/AzFitMkPMSU*>.

No decorrer deste curso você entenderá onde e como essa tecnologia pode ser utilizada com vantagem em relação ao que se teve até hoje.

O que garante a segurança das transações em ambientes que usam a tecnologia *blockchain* é a criptografia assimétrica (de chaves públicas) e recursos relacionados, que você vai entender melhor no tópico a seguir.

Como a segurança da informação é garantida na *blockchain*

Uma transação realizada entre duas partes em um ambiente ou aplicação que usa *blockchain* pode garantir a segurança e a confiabilidade de várias maneiras, todas elas por meio do uso da criptografia assimétrica e da assinatura digital.

Segundo o CERT.BR (2012), a criptografia (ciência de escrever mensagens em forma cifrada) de chaves assimétricas ou criptografia de chave pública, permite cifrar os dados de uma transação utilizando duas chaves distintas: uma pública que pode ser livremente divulgada, e uma privada que deve ser mantida em segredo. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade, ou autenticação, integridade e não repúdio, conceitos definidos a seguir.

- **Confidencialidade:** A confidencialidade é conseguida quando quem inicia a transação (emissor) utiliza a chave pública de quem vai receber a transação (receptor) para criptografá-la. Ao receber a transação, o receptor utiliza sua chave privada (que é secreta e somente

ele tem posse) para descriptografá-la. Como somente o receptor tem a chave privada capaz de decodificar a transação, isso garante que a transação foi confidencial e que nenhuma outra pessoa além do receptor pôde decifrá-la. Se alguém interceptar a informação, não conseguirá decifrá-la, pois não tem a chave privada necessária para isso.

Exemplo: Esse processo pode ser usado no envio de uma determinada quantidade de criptomoeda para outra pessoa em uma transação. Para enviar as criptomoedas, você utiliza o endereço de *wallet* do receptor, que é a chave pública dele. Ao receber a transação, somente esse receptor possui a chave privada necessária para decifrá-la e, assim, aproveitar os valores em criptomoeda envolvidos.

- **Autenticidade:** A autenticidade é conseguida quando quem inicia a transação (emissor) utiliza sua chave privada (e secreta) para criptografá-la de modo a garantir a autoria ou sua identificação em uma transação. Quem recebe o conteúdo da transação (receptor) poderá descriptografá-lo, pois tem acesso à chave pública de quem a enviou (emissor). Qualquer outra pessoa que tem a chave pública do emissor poderá decifrar a transação, que pode ser considerada autêntica por ter sido cifrada com a chave privada do emissor.
- **Integridade:** A integridade dos dados é garantida pelo uso da função de hash que gera um resumo criptográfico de tamanho fixo da informação a ser enviada ou armazenada. Esse resumo pode ser comparado a uma impressão digital e, uma vez gerado, não pode ser alterado. Caso qualquer alteração seja feita na informação durante a transmissão ou armazenamento, um novo resumo totalmente diferente é gerado, permitindo detectar que a informação foi alterada e, se necessário, rejeitar tal alteração.

  Exemplo: Em um ambiente de *blockchain*, cada bloco, contendo centenas de transações, tem gerado um resumo (*hash*) de tamanho único, quando este bloco é gravado. Depois de gravado,

qualquer alteração no bloco gerará um resumo totalmente diferente, permitindo detectar que o bloco foi alterado, o que o invalidaria, já que a alteração poderia ser feita por um criminoso virtual ou por uma das partes envolvidas, em benefício próprio.

- **Não repúdio:** O não repúdio é um conceito que busca evitar que uma entidade possa negar que foi ela quem executou uma ação.
- **Assinatura digital:** A assinatura digital é conseguida pelo uso conjunto da criptografia assimétrica para garantir a autenticidade e da função de *hash* para garantir a integridade dos dados. Quando se diz que uma transação foi assinada digitalmente, significa que quem originou a transação (emissor) gerou um resumo (*hash*) do conteúdo dessa transação e o criptografou com sua chave privada, anexando-o ao conteúdo da transação, também criptografada. Em seguida, enviou a transação com o resumo criptografado para a outra parte (receptor). Ao receber a transação, o receptor calcula um novo resumo (*hash*) e descriptografa o resumo e a transação recebidos utilizando a chave pública do emissor. Se o resumo recebido for igual ao resumo calculado, a informação está íntegra, o que significa que não sofreu alteração na transmissão. Caso sejam diferentes, a assinatura está incorreta, o que significa que pode ter havido alterações na transação. O processo de assinatura digital pode ser visto na figura 1.

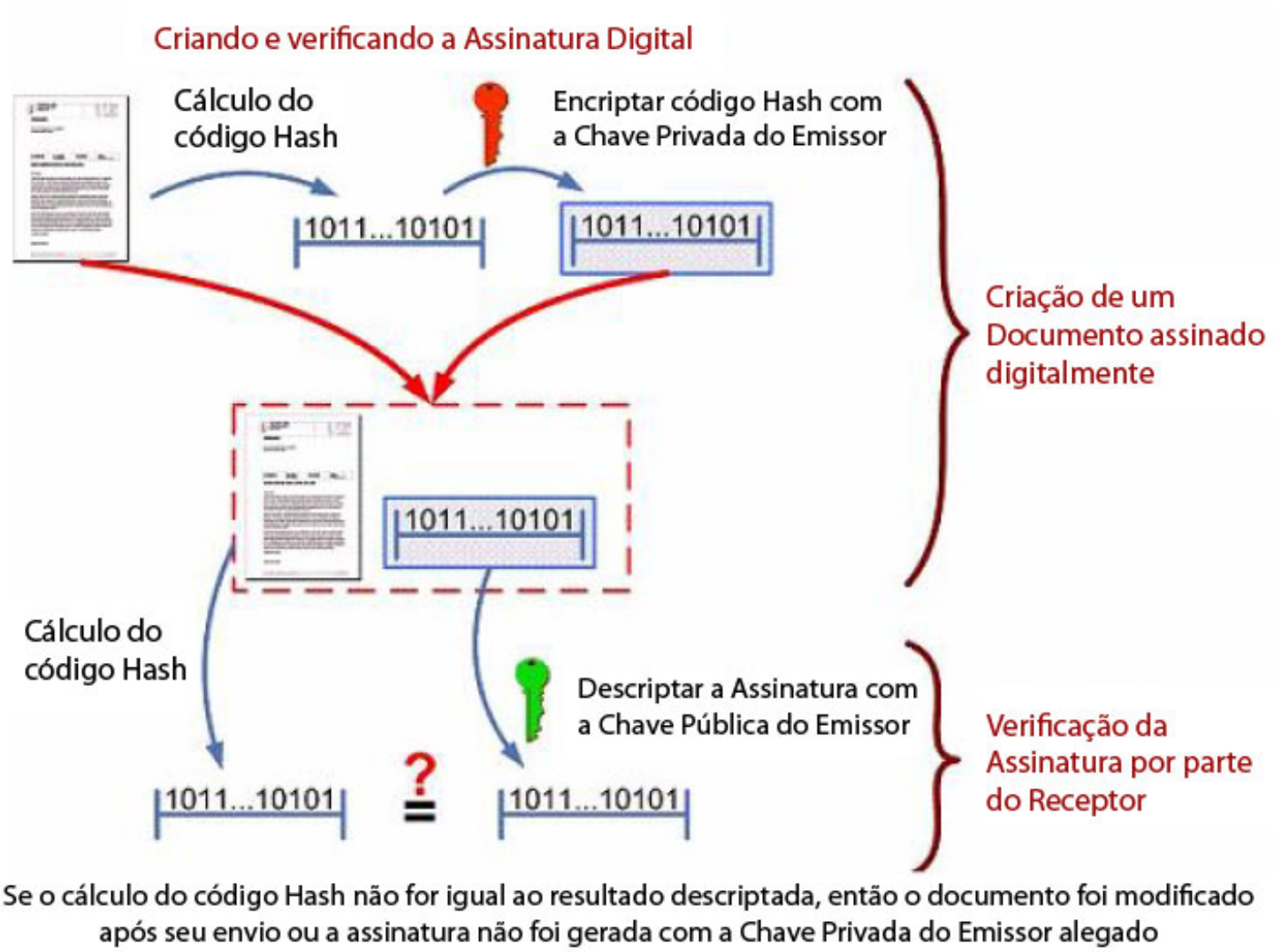

Figura 1 – Assinatura Digital

Fonte: *https://www.gta.ufrj.br/grad/07_1/ass-dig/ComocriarumaAssinaturaDigital.html*

Principais áreas de uso da tecnologia *blockchain*

Uma vez que a tecnologia *blockchain* permite transações confiáveis entre partes sem precisar de uma autoridade central entre elas, e que as transações podem ser rastreadas da origem ao destino de forma transparente, seu uso pode se dar em várias áreas, sendo as principais delas contratos inteligentes, criptomoedas e DApps - Decentralized Applications.

- **Contratos inteligentes** (***smart contracts***): Segundo a Exchange Binance, a tecnologia *blockchain* é a base dos contratos inteligentes. Basicamente cria-se uma rede que usa *blockchain* e possui diversos nós descentralizados que se encarregarão de validar as transações envolvidas nos contratos inteligentes. Esses contratos utilizam protocolos trustless, ou seja, não exigem terceiros confiáveis para intermediar as transações. Isso significa que duas partes podem fechar um contrato por meio da *blockchain* sem ter que se conhecer ou confiar uma na outra. Um contrato

inteligente garante que, se as condições do contrato não forem cumpridas, o contrato não será executado, mas se forem cumpridas, será executado de forma confiável. Muitos visionários preveem que os contratos inteligentes poderão eliminar entidades centralizadas de validação de confiança como cartórios, bancos, entidades de controle etc. Os mais entusiastas preveem, inclusive, a independência do cidadão em relação ao estado.

Como os contratos inteligentes precisam de uma rede de *blockchain* para serem executados e os custos gerados precisam ser pagos de alguma forma, as redes de diversas criptomoedas estão sendo utilizadas para criar esses contratos, sendo a principal delas a rede Ethereum (*https://www.ethereum.org*/), cuja criptomoeda associada é a Ether (ETH). Mesmo a rede Bitcoin pode ser usada para executar contratos inteligentes, mas não se tornou muito popular nesse aspecto. Um contrato inteligente executado na rede Ethereum tem os custos pagos por meio da criptomoeda Ether (ETH), impulsionando o uso da criptomoeda e a valorizando no mercado. Há diversas outras plataformas de *blockchain* de criptomoedas que podem ser utilizadas para executar contratos inteligentes.

Saiba mais

Entenda o que são e como funcionam os contratos inteligentes (*smart contracts*): <*https://youtu.be/g29IrXcBDGU*>.

Saiba mais

Caso de uso de um contrato inteligente fictício na rede Ethereum

Paulo deseja vender seu carro. Então ele entra na rede Ethereum e cria seu endereço de *wallet* (*public key*) na *blockchain* Ethereum e obtém uma chave privada (*private key*). Em seguida, cria um *smart contract* e define os termos da venda, assinando o contrato com sua chave privada (*private key*). Então ele deixa o carro em uma *garage locker* (garagem trancada eletronicamente) onde seu carro também possui um endereço na *blockchain* Ethereum.

Marcos vê o anúncio na internet e se interessa pelo carro de Paulo. Então ele assina o contrato com sua *public key* (endereço de *wallet* Ethereum) transferindo o valor pedido por Paulo, em Ether (ETH), para a *wallet* de Paulo. O *smart contract* assinado é enviado para a rede *blockchain* para ser validado. Um dos mineradores (nós) da rede Ethereum ganha o direito de validar o contrato, verificando os dados para saber se todas as regras foram seguidas e se Marcos tem criptomoedas (ETH) suficientes para pagar Paulo. Se todos os nós da rede concordarem que as regras foram seguidas, Marcos recebe o código de acesso ao *garage locker* onde está o veículo e seus dados são registrados na *blockchain* como novo proprietário do veículo. Então, Marcos vai até o *garage locker* e desbloqueia o carro, que agora é seu.

- **Criptomoedas:** Para viabilizar o uso de uma criptomoeda é criada uma rede distribuída (*blockchain*) que respeita um conjunto de protocolos (regras) envolvendo os recursos de criptografia apresentados anteriormente. Nessa rede, centenas de transações realizadas entre pessoas são colocadas em um bloco e validadas por centenas ou milhares de computadores, chegando-se a um consenso que determina se as transações são válidas ou não. Se as transações do bloco forem consideradas válidas, o bloco é gravado na

rede *blockchain* da criptomoeda e tais transações são registradas em uma espécie de “livro-razão” chamado de *ledger*. Qualquer pessoa ou aplicação poderá ter acesso a esse *ledger* e rastrear a transação desde sua origem. A figura 2 mostra o formato de um bloco que conterá centenas de transações.

Figura 2: Formato do bloco

Fonte: Senai - Serviço Nacional de Aprendizagem Industrial.

A figura 3 mostra a interligação dos blocos na *blockchain*.

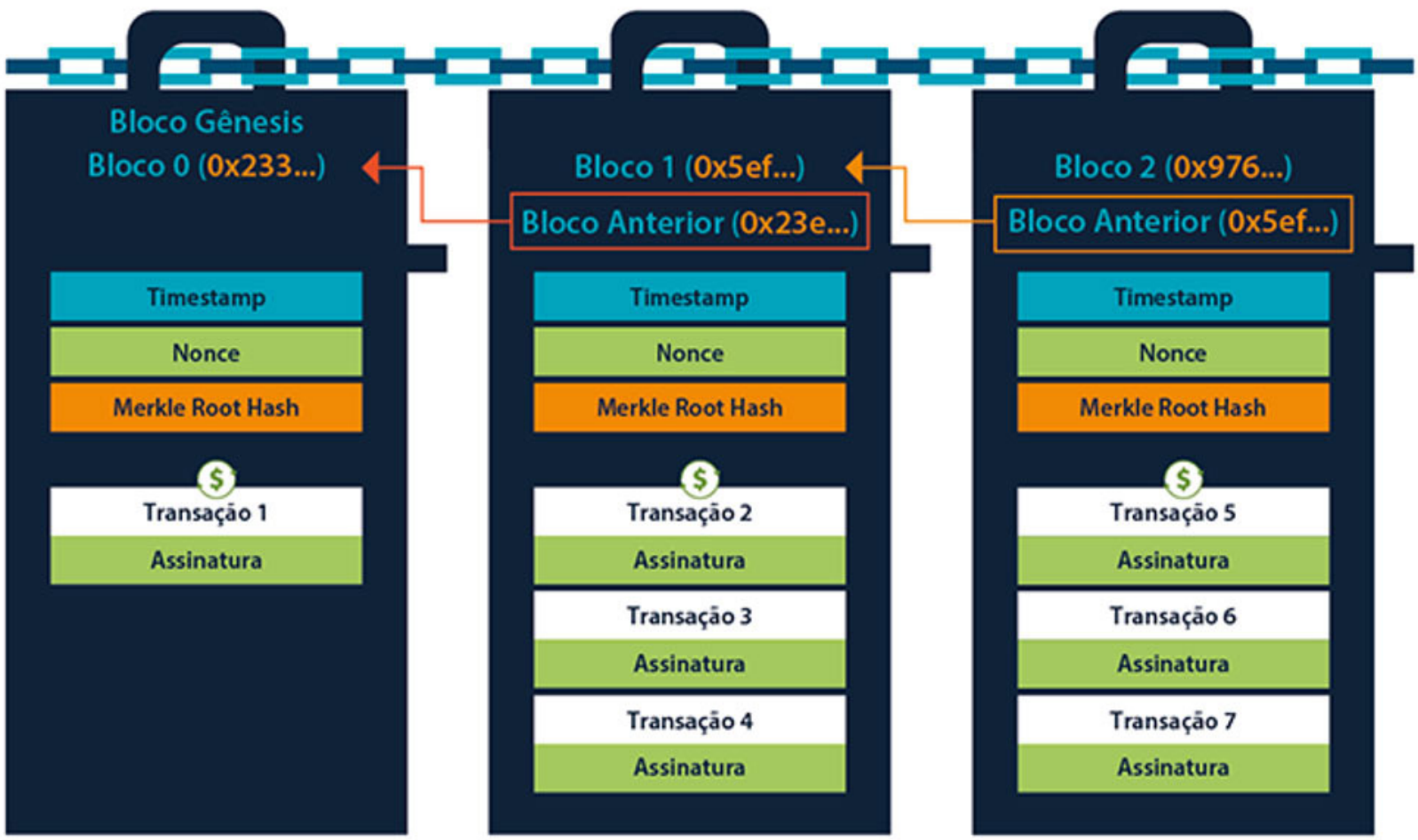

Figura 3: Interligação de blocos na *Blockchain*

Fonte: Senai - Serviço Nacional de Aprendizagem Industrial.

O bloco gravado é espelhado automaticamente para milhares de computadores que participam da rede *blockchain*. Assim, para um criminoso virtual conseguir alterar transações teria que fazer em milhares de computadores. Além disso, como os blocos são interligados na *blockchain*, alterar um bloco impactaria em disseminar essa alteração para todos os demais blocos gravados a partir dele, uma tarefa praticamente impossível nos dias atuais.

Cada bloco inserido na *blockchain* aponta para o bloco anterior por meio de um código *hash* (resumo do bloco) que identifica exclusivamente cada bloco para evitar alteração. Assim, as transações na *blockchain* podem ser rastreadas desde o bloco inicial da cadeia, chamado de **bloco g**ênesis.

A figura 4 mostra como é formada a cadeia de blocos a partir do bloco gênesis.

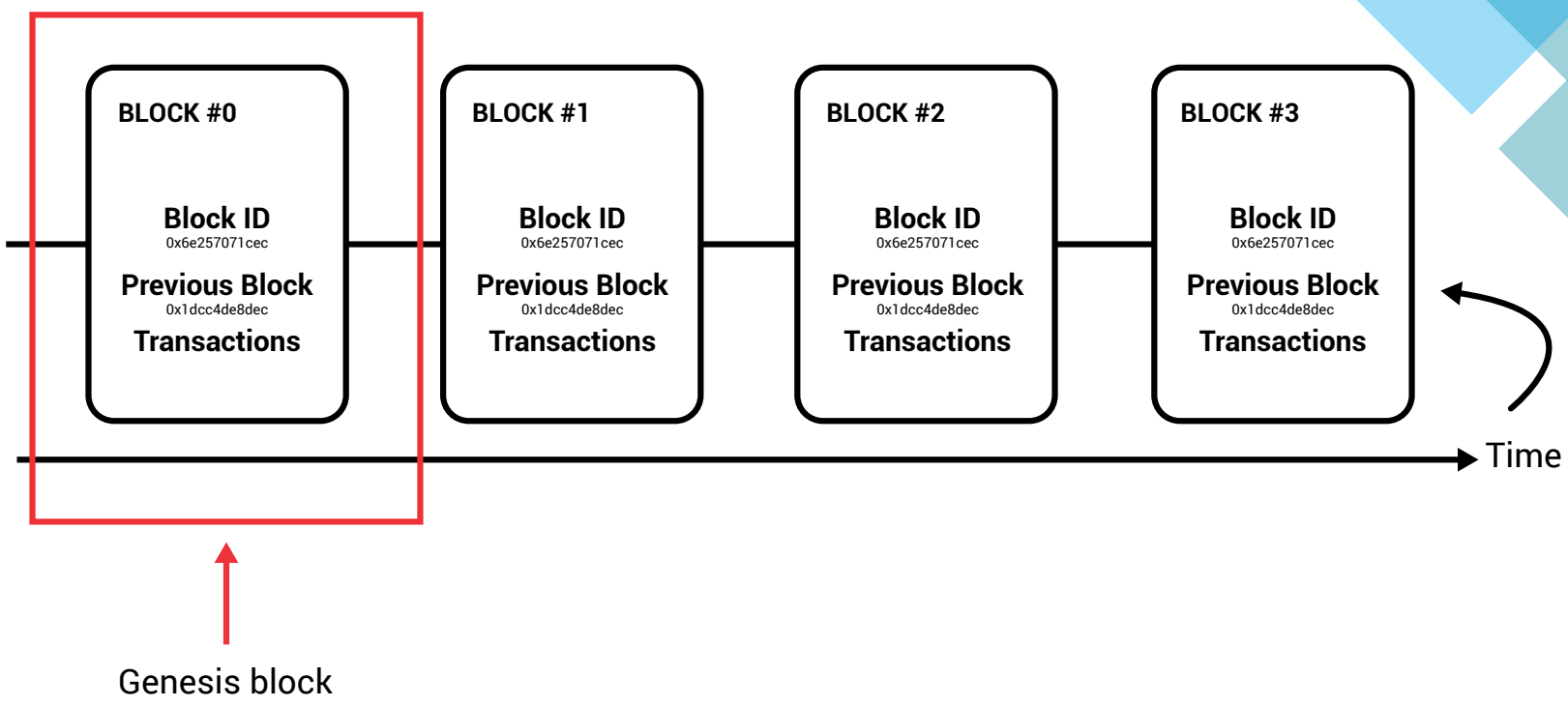

Figura 4: *Blockchain*.

Fonte: <*https://medium.com/coinmonks/how-to-create-your-own-private-ethereum-blockchain-137ab15989c6*>.

Observe que o bloco seguinte sempre aponta para o bloco anterior, ou seja, contém o *hash* do bloco anterior, formando a cadeia de blocos (*blockchain*).

Você pode entender a *blockchain* como uma rede que contém um banco de dados distribuído para se armazenar blocos (contendo centenas de transações) e um livro-razão (*ledger*) para registro das transações.

Quando se faz uma transação com criptomoeda, está garantido o anonimato entre as partes e a descentralização. A descentralização ocorre porque não é necessária uma autoridade central para

atestar que a transação é autêntica. A autenticidade é conseguida por meio dos recursos de criptografia assimétrica. Já o anonimato é garantido porque você não precisa saber o nome ou documento da pessoa com quem vai realizar a transação. Precisará saber apenas o endereço de *wallet* da pessoa para a qual vai enviar as criptomoedas. Esse endereço de *wallet* é a chave pública da pessoa, que será usada para criptografar a transação.

Saiba mais

No site <*https://coinmarketcap.com/*> você pode obter informações sobre as 2.928 criptomoedas registradas até a data de produção deste material (2/10/2019).

Veja na figura 5 quanto cada uma das principais criptomoedas ocupa do total do mercado.

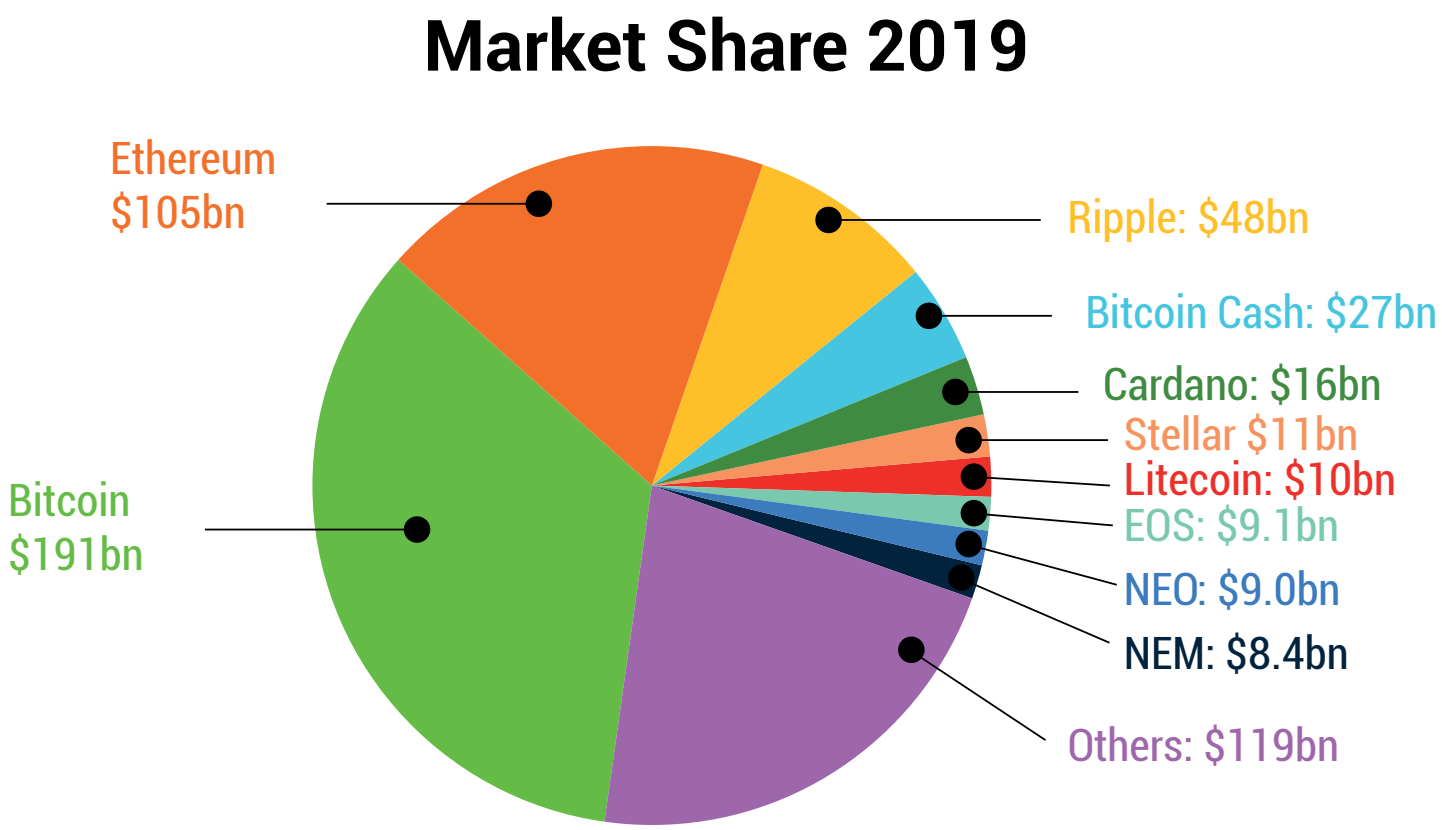

Figura 5 – Criptomoedas mais usadas no mundo

Perceba que Bitcoin (BTC), Ether da rede Ethereum (ETH) e Ripple (XRP) representam mais da metade de toda a movimentação com criptomoedas. Como você pode observar, o mercado de criptomoedas hoje movimenta mais de 550 bilhões de dólares.

- **DApps - Decentralized Applications:** são aplicativos executados em uma rede de computadores P2P (que permite transações pessoa-pessoa) em vez de executar em um computador central. Isso permite que o aplicativo seja executado na internet sem ser controlado por uma única entidade. Basicamente você pode entender DApps como aplicativos que executam em ambiente de *blockchain*, ou seja, aplicativos que executam de forma descentralizada, normalmente não estando ligados a um servidor ou entidade central.

  Todas as criptomoedas existentes hoje são DApps, pois são softwares que permitem transações criptografadas e descentralizadas, registradas na *blockchain*. Mas DApps vão além. Há aplicativos desenvolvidos em *blockchain* que permitem rastrear a cadeia de suprimentos, desde a origem da matéria-prima até o produto final industrializado. Há jogos desenvolvidos com conceito DApp em *blockchain*, em que os dados são armazenados na cadeia de blocos e as negociações financeiras são realizadas com criptomoedas. As próprias eleições no Brasil poderão ser realizadas por meio de DApp, permitindo registro imutável do voto, rastreabilidade e acompanhamento de resultados em tempo real. Há muitas aplicações para desenvolvimento de aplicações de forma descentralizada.

PROCESSO DE VALIDAÇÃO DE TRANSAÇÕES COM CRIPTOMOEDAS – POW E POS

Para que um bloco de transações seja gravado na *blockchain,* deve haver o que chamamos de consenso, onde milhares de computadores participantes da rede *blockchain* concordam que as transações do bloco foram verificadas e validadas. O consenso pode ser conseguido pelo uso de mecanismos diferentes, sendo os principais deles chamados de **Proof-of-Work (PoW)** e **Proof-of-Stake (PoS)**.

Saiba mais

Veja no vídeo a seguir um resumo dos mecanismos de consenso PoW e PoS: <*https://youtu.be/04uds1SyAAU*>.

Proof-of-Work (PoW)

Para entender como funciona o sistema Proof-of-Work (PoW) (prova de trabalho) você precisa entender como funciona uma transação envolvendo criptomoedas. Quando você envia uma quantidade de criptomoeda para o endereço de wallet (chave pública) de outra pessoa, a transação é enviada para a rede da criptomoeda e os milhares de computadores que compõem a rede competem para validar a transação e montar um bloco com esta e outras transações. Estes computadores são chamados mineradores.

Para conseguir montar um bloco, esses mineradores precisam encontrar um código de *hash* disponibilizado em segredo pela rede, que identificará o bloco que será gravado. Esse processo exige milhões de operações lógicas (comparações) para descobrir o código correto. Isso faz com que os computadores com maior poder de processamento tenham mais chances de encontrar o código e ganhar o direito de validar e gravar o bloco na *blockchain*. O minerador que consegue descobrir o código *hash* primeiro, valida ("checa") as transações e após os demais mineradores verificarem se ele realmente conseguiu encontrar o código *hash* do bloco, grava o bloco e registra as transações no *ledger* (livro-razão). Por esse trabalho o minerador ganha novas unidades da moeda que são geradas e registradas em novas transações na *blockchain*.

Na rede Bitcoin, por exemplo, um minerador que ganha o direito de gravar um bloco recebe, na data de confecção deste material, 12,5 Bitcoin, o que equivale a R$ 103.205,75.

Quando todos os mineradores concordarem e darem o direito ao minerador que encontrou o *hash* do bloco de validar as transações e gravar o bloco na *blockchain,* ocorre o que chamamos de **consenso** usando o mecanismo Proof-of-Work, em que há um trabalho intenso de processamento.

Por ser muito difícil conseguir sozinho poder de processamento para descobrir o *hash* que permitirá validar e gravar um bloco, os mineradores normalmente unem seus poderes de processamento em *pools* de mineração. Um *pool* é um site onde mineradores podem associar-se a outros mineradores unindo seus poderes de processamento como se fossem um único supercomputador, trabalhando juntos para achar o *hash* do bloco. Quando acham o *hash*, dividem entre si as recompensas.

Proof-of-Stake (PoS)

Enquanto no sistema de validação de transações Proof-of-Work (PoW) máquinas com grande poder de processamento competem entre si na rede da criptomoeda para encontrar um código *hash* que permitirá validar e gravar o bloco de transações na *blockchain*, no sistema Proof-of-Stake (PoS) você não precisa de máquinas poderosas, mas sim deixar uma quantidade da criptomoeda congelada na sua *wallet*, em um computador comum, celular, *wallet* na web etc.

Proof-of-Stake pode ser traduzido como Prova de Participação, ou seja, o seu montante congelado na *wallet* determina o seu poder de participação e chance de validação de bloco na rede daquela criptomoeda.

Wallet é um *software* que permite guardar suas criptomoedas. Nesse *software* você terá um ou mais endereços de *wallet* da moeda. Endereço de *wallet* é o endereço que identifica o local onde se guarda uma criptomoeda e para o qual as pessoas enviam criptomoedas para você. Nada mais é do que um endereço codificado no sistema hexadecimal, algo como o endereço de Bitcoin 1Hz96kJKF2HLPGY15JWLB5m9qGNxvt8tHJ ou o endereço de Ether 0x709bc24ef6d6d22a02f315ff5bfb42b9888f88b4 da rede EThereum.

No método de validação de transações Proof-of-Stake (PoS) quem vai validar o bloco de transações é escolhido aleatoriamente por um algoritmo que considera o tempo em o dono da *wallet* vai manter as moedas congeladas, a quantidade de moedas congeladas etc. O que o algoritmo vai considerar muda em cada criptomoeda, de acordo com características particulares. Quanto maior o montante em *stake* (congelado), maiores são as chances de ser escolhido para validar um bloco.

Saiba mais

Veja no link a seguir um vídeo mostrando como funciona o sistema de validação Proof-of-Stake (PoS):

<*https://www.binance.vision/pt/blockchain/proof-of-stake-explained*>.

Enquanto no sistema Proof-of-Work (PoW) dizemos que os blocos são "minerados", no sistema de Proof-of-Stake (PoS) dizemos que os blocos são "forjados". As criptomoedas que adotam o sistema PoS como método de validação, normalmente, começam vendendo algumas unidades que foram geradas previamente ou então são lançadas como PoW e, depois, mudam para PoS.

No sistema PoW os mineradores são recompensados com novas moedas que são geradas e no sistema PoS eles são recompensados com as taxas cobradas nas transações.

Com a inviabilização da mineração doméstica de criptomoedas que usam o sistema PoW devido à queda dos preços a partir de meados de 2018 e, devido ao alto preço da energia elétrica no Brasil, pessoas passaram a participar do processo de validação PoS para receber um rendimento extra para incrementar o orçamento doméstico.

USABILIDADE DAS CRIPTOMOEDAS

No aspecto técnico, uma criptomoeda é um *software* de computador que respeita um conjunto de regras (protocolos) e executa em centenas (ou milhares) de computadores pelo mundo de forma distribuída e sincronizada. Sim, uma criptomoeda é um *software* cuja segurança dos dados é garantida pela criptografia.

O Bitcoin (BTC) foi a primeira criptomoeda inventada, por volta de 2009, mas atualmente já quase 3 mil criptomoedas registradas (ver no site <*https://coinmarketcap.com/*>.)

Saiba mais

Veja o *whitepaper* (projeto) do Bitcoin no link: <*https://bitcoin.org/bitcoin.pdf*>.

Problemas que impactam no uso das criptomoedas

Apesar do número crescente de criptomoedas, sua utilização ainda é modesta, pois a própria natureza da tecnologia *blockchain* enfrenta um conjunto de barreiras, como a limitada escalabilidade (dificuldade de uso se o número de usuários aumentar exponencialmente), necessidade de alto poder computacional, falta de regulamentação do Estado, complexidade de uso e demora para concluir a transação. Vamos entender estes problemas a seguir.

- **Limitada escalabilidade:** O problema de escalabilidade se refere à quantidade de transações que a rede de uma criptomoeda pode processar em uma unidade de tempo. Blocos na *blockchain* são limitados em tamanho e frequência. Por exemplo, na rede Bitcoin, a capacidade de processamento de transações da rede é limitada pelo tempo médio de criação de blocos de 10 minutos e pelo limite de tamanho de bloco de 1 megabyte (MB). A capacidade máxima de processamento de transações estimada usando um tamanho médio ou mediano de transações está entre 3,3 e 7 transações por segundo. Imagine se aumentasse exponencialmente o número de pessoas utilizando Bitcoin. Certamente a rede não suportaria ou os tempos de transações seriam inviáveis. Muitas criptomoedas foram criadas para tentar resolver o problema da escalabilidade da *blockchain*, como as criptomoedas Zilliqa (ZIL) e QuarkChain (QKC). Para a rede Bitcoin a proposta mais avançada para resolver o problema da escalabilidade está na criação de uma rede de apoio chamada Lightning Network (LN).
- **Necessidade de alto poder computacional:** Para validar transações com criptomoedas que usam o sistema de validação (consenso) Proof-of-Work, são necessários equipamentos cada vez mais potentes na medida que a dificuldade de mineração (validação) aumenta com o passar do tempo. Segundo Galeon (2017), estimava-se, em 2017, que

a energia elétrica gasta para validar transações com Bitcoin era equivalente à energia consumida por cerca de 159 países do mundo. Os clamores pela sustentabilidade do planeta têm levado a comunidade internacional a pressionar pelo desenvolvimento e uso de mecanismos de validação de transações com criptomoedas que não exijam tamanho esforço computacional e consequente consumo elevado de energia. Isso levou ao surgimento de outros mecanismos de consenso como Proof-of-Stake (PoS), apresentado em tópico anterior.

- **Falta de regulamentação:** Apesar de alguns esforços já estarem sendo feitos no Brasil e no mundo, ainda estamos longe de regular o uso das criptomoedas, fazendo com que criminosos usem esse mercado para lavar dinheiro e executar todo tipo de transação ilícita envolvendo valores financeiros. A criação de pirâmides financeiras (esquemas Ponzi) e empresas fraudulentas têm sido comuns, atraindo pessoas com promessas de lucro fácil e rápido. No Brasil a Instrução Normativa RFB nº 1.888, de 3 de maio de 2019 institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). Na Câmara dos Deputados tramita o Projeto de Lei (PL nº 2.303/2015) que discute a aprovação da inclusão das moedas virtuais e programas de milhagem aéreas na definição de "arranjos de pagamento" sob a supervisão do Banco Central do Brasil.

Saiba mais

Instrução Normativa RFB nº 1.888 de 3 de maio de 2019.

<*https://www.legisweb.com.br/legislacao/?id=377332*>.

Projeto de Lei (PL nº 2.303/2015)

<*https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1555470*>.

- **Complexidade de uso e demora para concluir a transação:** Para quem está acostumado a pagar compras de qualquer valor com cartão de crédito ou débito em segundos vai estranhar a execução de compras usando criptomoedas. Primeiro porque uma transação com Bitcoin, por exemplo, pode levar de 10 a 20 minutos para ser completada. Segundo, porque para pagar algo com criptomoeda você precisa enviar uma determinada quantidade de criptomoeda da sua wallet (no celular, computador ou web) para um endereço de criptomoeda da outra pessoa ou empresa. Você teria que enviar Bitcoin, por exemplo, para o endereço 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX, difícil de digitar e memorizar. Apesar de haver recursos como QR Code para apresentar os endereços de envio sem a digitação do endereço complexo, ainda estamos longe de um sistema de pagamentos que se aproxime do que temos hoje com cartões de crédito ou débito.

PRINCIPAIS CRIPTOMOEDAS

Diferença entre criptomoedas e FIAT Money

Diariamente utilizamos a moeda corrente do nosso país, no nosso caso, o real (R$). A moeda corrente é conhecida como moeda FIAT (FIAT Money), traduzida como moeda fiduciária.

Moeda fiduciária pode ser definida como qualquer título não-conversível, ou seja, que não é lastreado a nenhum metal (ouro, prata) e não tem nenhum valor intrínseco. Seu valor advém da confiança que as pessoas têm em quem emitiu o título. A moeda fiduciária pode ser uma ordem de pagamento (cheques, por exemplo), títulos de crédito, dinheiro de papel, entre outros.

Quando usamos o real ou o dólar, temos confiança no governo que emitiu essas moedas, mesmo sabendo que não há lastro em ouro, por exemplo. Uma moeda que possui lastro significa que você tem o equivalente à quantidade emitida da moeda em um metal precioso, como o ouro. As moedas emitidas por muitos países já tiveram lastro em ouro no passado, mas hoje há uma quantia infinitamente maior no mercado do que a quantidade de ouro em poder do Estado. Assim, as moedas atuais, na maioria dos casos, não são mais lastreadas.

O grande problema das criptomoedas hoje é justamente a confiança em quem as emite. Não é um Banco Central, não é um Estado, não é um órgão de controle. São empresas, grupos de pessoas, sem nenhum controle de órgãos reguladores. Isso faz com que golpistas (*scammers*) criem criptomoedas atreladas a projetos falsos com objetivo único e exclusivo de enriquecer vendendo essas criptomoedas com a promessa de que irão valorizar quando o falso projeto for executado em algum nicho de negócio real.

A criptomoeda não é considerada uma moeda FIAT porque não advém, na maioria das vezes, de origem que permita alto nível de confiança. O Bitcoin, por exemplo, é mantido por uma comunidade de pessoas que mantém e atualiza a rede, concentrando as informações no site <*https://bitcoin.org/en/*>. Não é mantido ou regulamentando por nenhum Estado ou órgão de controle. A confiança que se têm no Bitcoin advém da confiança na equipe que mantêm a rede.

Em diversas partes do mundo já existem máquinas que funcionam como caixas eletrônicos permitindo que você saque criptomoedas recebendo em moeda FIAT. Nessas máquinas você pode depositar dólar, por exemplo, em uma *wallet* de Bitcoin. Ou seja, nessa transação você compra

Bitcoin com dólar e recebe na sua conta (*wallet*) de Bitcoin. O contrário também é possível. Você pode sacar Bitcoins e receber em dólar. Nessa transação você vende os Bitcoins (ou troca) por dólar.

Saiba mais

Veja o vídeo que mostra máquinas ATM que funcionam como caixas eletrônicos onde você pode trocar Bitcoin por dólar e vice-versa.

<*https://youtu.be/WbdQ-Q00dFY*>.

Há também cartões, como cartões de crédito, que você atrela a sua conta (*wallet*) da criptomoeda, de forma que você paga contas em dólar, por exemplo, sendo debitado o valor equivalente do seu saldo na sua *wallet* de criptomoeda. Esses serviços estão se tornando cada vez mais comuns, mas as taxas de conversão de moeda FIAT para criptomoeda e vice-versa ainda são muito altas, normalmente superiores às taxas cobradas em transações bancárias tradicionais. Alguns dos cartões mais utilizados são o cartão BitPay Visa, Shift Payments Coinbase, Wirex Visa, CryptoPay e Crypto.com. A figura 6 mostra o cartão de Bitcoin.

Figura 6: Cartão para débito de Bitcoin

Fonte: *https://news.bitcoin.com/8-crypto-debit-cards-you-can-use-around-the-world-right-now/*

As mais de 2.941 criptomoedas existentes hoje estão registradas no site CoinMarketCap, que traz informações atualizadas sobre as criptomoedas registradas. Neste site as criptomoedas são ranqueadas por grau de importância, estando na primeira página as principais criptomoedas.

Saiba mais:

Veja as criptomoedas registradas no site do CoinMarketCap no link: <*https://coinmarketcap.com/*>.

Diferenças entre criptomoedas e tokens

Criptomoedas e *tokens* são termos semelhantes. Ambos são ativos financeiros com representação em ambientes computacionais de *blockchain* e que possuem um valor no mundo real, sendo comercializadas em corretoras (*exchanges*). A diferença fundamental é que uma criptomoeda possui uma rede *blockchain* própria, e um *token* não.

A plataforma Ethereum, por exemplo, permite criar *tokens* usando o protocolo ERC-20 e a rede de *blockchain* da Ethereum. É muito comum você encontrar a referência a *tokens* ERC-20, o que significa que são *tokens* criados na plataforma de *blockchain* da Ethereum e que vão ser utilizados usando a rede *blockchain*.

Bitcoin (BTC), Litecoin (LTC), Ethereum, Dash, Monero (XMR) e ZCash (ZEC), são consideradas criptomoedas, pois possuem sua própria rede

blockchain. Já Blockstack (STX), Perlin (PERL), Telegram (TON), Algorand (Algo) Bitsdaq (BQQQ), Coti (COTI), Matic Network (MATIC), Metronome (MET) etc., são *tokens* criados em plataformas de *blockchain* existentes.

Além da plataforma Ethereum, há dezenas de outras plataformas que permitem a criação de *tokens* em poucos minutos, como a Stellar, NEO, EOS, Waves, TRON etc. *Tokens* criados na plataforma NEO usam um protocolo chamado NEP-5. *Tokens* criados na plataforma TRON usarão o protocolo TRC-20. Lembrando que um protocolo é um conjunto de regras que precisam ser seguidas por quem vai criar o *token* na plataforma.

Como criar uma rede *blockchain* demanda tempo e grande grau de conhecimento técnico, a maioria das empresas ou pessoas que desejam criar uma criptomoeda, o fazem na forma de *token*, em uma plataforma segura, confiável e consolidada. Para criar *tokens* em uma plataforma existente, é necessário pagar pela criação do *token* usando a criptomoeda oficial da plataforma. Assim, para você criar um *token* na plataforma Ethereum, terá que pagar usando a moeda Ether (ETH).

Apesar de haver uma distinção quanto ao ambiente em que a moeda virtual irá executar, ambos são referenciados, de modo geral, como criptoativos, mas convencionou-se chamar todos de criptomoedas. É mais comum ouvirmos o termo criptoativos para referenciar todas as categorias de ativos de valor no mundo da criptografia, como criptomoda, *tokens*, security tokens, *real state tokens*, *stablecoins* etc.

Para fins de padronização, usaremos neste curso o termo criptomoeda para referenciar a qualquer ativo digital do mundo da criptografia.

Principais criptomoedas

A seguir vamos listar as principais criptomoedas e suas características.

- **Bitcoin (BTC):** O Bitcoin (BTC) é sem dúvida a principal criptomoeda hoje, concentrando sozinho quase metade dos investimentos em criptomoedas no mundo.
  No preço atual (em 4/10/2019) de $ 8.183,20, desde que foi lançado o BTC, valorizou cerca de 5.948,19%, enriquecendo milhares de pessoas que acreditaram no projeto inicial e adquiriram Bitcoin a centavos de dólar.
  O máximo de BTC que a rede Bitcoin poderá emitir é 21.000.000 de BTC, tendo sido emitidos até hoje, por meio da mineração PoW, 17.973.887 BTCs, o que equivale a cerca de $147.083.842.708 USD.
  O principal motivo pelo qual as pessoas adquirem BTC é como investimento contando com valorização futura, uma vez que quando o total de BTCs forem emitidos (21.000.000) acredita-se que a oferta será bem menor que a procura, elevando os preços a patamares ainda não alcançados. No universo das criptomoedas compara-se o Bitcoin ao ouro no mundo real. Pessoas adquirem BTC devido à mesma busca de segurança que se tem no ouro.
  Hoje já foram emitidos 17.973.887 BTCs, restando apenas 3.026.113 BTCs para serem minerados (gerados).
- **Ethereum:** A plataforma Ethereum permite que programadores possam criar suas próprias criptomoedas (nesse caso, chamadas de tokens) usando a rede Ethereum, sem precisar criar uma nova *blockchain*.
  Também permite que sejam criados contratos inteligentes, para permitir negociações de produtos ou serviços sem uma entidade central para impor confiança na negociação.
  Quando uma criptomoeda é criada na plataforma Ethereum, ela precisa seguir um protocolo da rede, conhecido como ERC-20, e ser programada usando uma linguagem de programação orientada a

objetos conhecida como *Solidity*. Como a criptomoeda criada não tem *blockchain* própria, é comum a chamarmos de *tokens* ERC-20, ou seja, criptomoeda criada na plataforma Ethereum usando o protocolo ERC-20.

Qualquer operação na rede Ethereum, como a criação de um *token* ou de um contrato inteligente, deve ser paga com a moeda oficial da plataforma Ethereum, conhecida como Ether (ETH). Assim, Ethereum é o nome da plataforma e Ether (ETH) é o nome da criptomoeda oficial da plataforma.

A vantagem de se criar uma criptomoeda (*token*) na plataforma Ethereum é que a plataforma é segura, madura e estável, já tendo sido testada em questões de segurança, disponibilidade e confiabilidade.

Criar a própria *blockchain*, além de ser uma tarefa árdua e exigir muita habilidade técnica, ainda pode deixar brechas de segurança que podem ser aproveitadas por criminosos virtuais. Assim, é mais vantajoso usar plataformas de *blockchain* confiáveis.

Hoje estão em circulação cerca de 108.015.751 ETH, a um preço de $176,42 USD por unidade de ETH, o que equivale a aproximadamente $19.055.737.352 USD. Não há um limite para a emissão de ETH, como ocorre com BTC.

Desde que foi lançada, a criptomoeda ETH já valorizou 6.130,22%. A Plataforma Ethereum é a segunda mais importante, atrás apenas da plataforma Bitcoin. Grande parte, senão a maioria das criptomoedas lançadas hoje, são criadas na plataforma Ethereum e, para tal, paga-se a criação com criptomoeda Ether (ETH), o que indica que essa criptomoeda sempre terá grande utilidade e, como tal, um bom lugar no *ranking* das principais criptomoedas.

Uma transação da rede Ethereum demora normalmente cerca de 1 a 5 minutos, enquanto uma transação na rede Bitcoin demora no mínimo 10 minutos.

A criptomoeda Ether (ETH) atualmente é minerada por equipamentos que possuem GPUs (RIGs) usando o sistema

Proof-of-Work (PoW), mas está previsto para o início de 2020 a validação de transações por meio do sistema Proof-of-Stake (PoS).

- **Ripple (XRP):** Ripple (XRP) é uma criptomoeda cuja transação é barata e é executada de forma segura em média de 4 segundos, por isso foi adotada como a criptomoeda preferida de algumas instituições financeiras e bancárias globais (cerca de 200 bancos e instituições de pagamento) para a transferência de fundos entre bancos. Dentre os bancos e instituições que realizam transações interbancos por meio da XRL estão American Express, Santander, Interbank, Ranco Rendimento, Istarem etc.
  O máximo número de unidades de XRP (*total supply*) que serão emitidas é 99.991.330.383 XRP e até hoje já foram emitidas 43.166.787.298 de XRP. Desde que foi lançada, a criptomoeda XRP já valorizou cerca de 4.597,81%.
  XRP foi criada e é controlada por uma companhia baseada em San Francisco, chamada Ripple. Não é uma moeda minerada e difere das demais criptomoedas porque a validação de transações é feita por nós confiáveis da rede Ripple, assim, não é considerada uma moeda com *blockchain* totalmente descentralizado.
  A XRP é uma criptomoeda consolidada e de eficiência e segurança já comprovadas, mas sua hegemonia nesse setor está sendo ameaçada pelo movimento das instituições financeiras e bancárias que sinalizam criar suas próprias criptomoedas. Um exemplo é o banco JP Morgan, que está criando a JPM Coin, uma criptomoeda considerada *stablecoin* porque terá um pareamento de 1:1 com relação ao dólar americano. Você pode saber mais no link <*https://www.jpmorgan.com/global/news/digital-coin-payments*>.
- **Litecoin (LTC):** Litecoin (LTC) é uma criptomoeda que foi criada com base no Bitcoin, em um hard fork ocorrido em 2011 por Charlie Lee, mas usando um protocolo de criptografia diferente chamado scrypt. É minerada por CPU (ASICs) no processo de validação

de transações Proof-of-Work (PoW). Hard fork é o termo que se usa quando, a partir da *blockchain* de uma criptomoeda, origina-se outra com características diferentes.
O máximo de LTCs que poderão ser emitidas é 84.000.000 LTCs e hoje já foram emitidas cerca de 63.418.729 LTCs.
Por ter concorrentes fortes como o Bitcoin (BTC) e devido à falta de transparência do projeto, que não tem um *whitepaper* (projeto) bem definido e nem um cronograma de evolução do projeto, Litecoin (LTC) vem perdendo espaço e sofrendo forte desvalorização nos últimos tempos.

- **Tether (USDT) e outras *stablecoins:*** Tether (USDT) é uma criptomoeda criada pela Exchange Bitfinex, que se enquadra na categoria de stablecoin. Diz-se que uma criptomoeda é stablecoin quando ela possui paridade com alguma moeda ou bem de valor do mundo real, como dólar, ouro etc. USDT possui paridade de 1:1 com o dólar americano. A Thether é a principal stablecoin utilizada hoje e foi a primeira criptomoeda criada nessa categoria.
Devido aos inúmeros processos movidos contra a mantenedora do Tether (USDT) por suspeitas de manipulação de mercado, esta criptomoeda vem perdendo força e abrindo espaço para outras *stablecoins*.
A Exchange Binance, por exemplo, uma das maiores corretoras de criptomoedas mundiais, lançou recentemente a *stablecoin* Binance USD (BUSD), também com paridade 1:1 com o dólar americano. Há pouco tempo essa mesma Exchange lançou a Binance GBP Stable Coin (BGBP), que tem paridade de 1:1 com a libra esterlina.

Saiba mais

Há outras *stablecoins* atreladas ao dólar, como a TrueUSD (TUSD), que você pode conhecer melhor no link <*https://www.trusttoken.com/*>. Há também o Paxos Standard (PAX) que você pode conhecer no link <*https://www.paxos.com/pax/*>, a USD Coin (USDC) com informações no link <*https://www.centre.io/usdc*>. e a Dai (DAI), com informações no link <*https://makerdao.com/pt-BR/dai*>.

Como não existe o dólar digital, quando alguém vai realizar uma operação com criptomoedas no mundo virtual é necessária uma representação para o dólar, e a representação mais aceita atualmente é o Tether (USDT).

Quando você vai fazer operações de *trade* (negociação) de criptomoedas como BTC, ETH, XRP, LTC etc., normalmente você troca seu saldo nessas criptomoedas por Tether (USDT) quando o preço sobe, pois USDT é estável e atrelada ao dólar. Depois, quando o preço da criptomoeda cai, você usa o seu saldo USDT para comprar uma quantidade maior. Por ser uma *stablecoin*, a USDT tem sido usada como uma representante do dólar no mundo virtual.

Em muitos casos, em algumas *exchanges* internacionais, se você tem outras criptomoedas, você precisa primeiro converter para USDT para depois transferir para sua conta bancária em dólar.

O MERCADO DE CRIPTOMOEDAS: COMPRA, VENDA, CRIAÇÃO E RISCOS

O primeiro passo para quem quer iniciar no mercado de criptomoedas é estudar o mercado e selecionar um grupo de criptomoedas que considera promissoras para investir. O Bitcoin é a criptomoeda principal e todas as demais são chamadas de *altcoins*.

Para saber se uma moeda é promissora vale a pena ler o *whitepaper* presente no site da criptomoeda, que detalha o objetivo da criptomoeda, o objetivo, usabilidade e agenda do desenvolvimento da tecnologia (*roadmap*) relacionada à criptomoeda. O *whitepaper* é algo semelhante ao plano de negócios da criptomoeda. Após ler o *whitepaper*, vale a pena pesquisar na internet a perspectiva da comunidade com relação àquela criptomoeda. Uma criptomoeda útil certamente terá boa aceitação da comunidade e tende a valorizar no futuro.

Saiba mais

Veja no vídeo como escolher uma criptomoeda promissora para investir: <*https://youtu.be/usP522cE1ms*>.

Riscos e oportunidades em operações de trade com criptomoedas

Como os preços das criptomoedas são muito voláteis, as possibilidades de lucro nas operações de *trade* são proporcionais às possibilidades de perdas.

Os preços são influenciados pela lei da oferta e procura, assim, maior procura das pessoas impacta no aumento do preço e, menor procura, na redução.

Dessa forma, os principais fatores que impactam nos preços são:

- cumprimento ou não do cronograma de evolução do projeto da criptomoeda (*roadmap*);
- notícias sobre regulamentação de criptomoedas;
- crises econômicas e guerras comerciais entre países;
- brigas internas em equipes mantenedoras de criptomoedas; e
- parcerias entre criptomoedas e empresas.

Assim, matemática e estatística são importantes para avaliar gráficos de evolução de preços, mas há muito mais que ciências exatas na definição dos preços das criptomoedas.

Nas operações de *trade*, em que os riscos são elevados, é sempre aconselhável utilizar uma estratégia chamada *stop loss* para conter possíveis prejuízos por quedas ou altas abruptas nos preços de uma criptomoeda em negociação.

Saiba mais

Veja no vídeo como usar a estratégia *stop loss* em uma operação de *trade* de criptomoedas: <*https://youtu.be/bIwZ5v80qCc*>.

Além de operações de *trade*, operadores do mercado de criptomoedas podem realizar arbitragem.

Arbitragem de criptomoedas é a realização da compra de uma criptomoeda em uma parte do globo onde o preço está mais baixo e a venda em outra parte onde o preço está mais alto.

Devido a fatores econômicos, a aceitação de criptomoedas pode ser maior ou menor por parte da população. Em países em crise econômica, onde a população perde confiança em sua moeda Fiat (moeda oficial) a população tende a procurar nas criptomoedas, principalmente no Bitcoin, uma alternativa. Já em países ricos, com moeda estável, a procura normalmente é menor. Assim, o preço das criptomoedas pode estar maior em países em crise financeira, propiciando lucros em operações de venda de criptomoedas compradas em *exchanges* de países ricos. Mas isso não é regra, já que a globalização permite que um cidadão comum negocie criptomoedas em *exchanges* situadas em qualquer país.

Saiba mais

Veja no vídeo como executar arbitragem com criptomoedas: <*https://youtu.be/uas7n-HHA30*>.

Como executar transações com criptomoedas de forma segura

O processo de transação com criptomoedas da origem até o destino tem a segurança garantida pela criptografia, porém o elo fraco nesse processo são os seres humanos envolvidos na transação, que podem ser vítimas de criminosos do mundo real ou virtual.

Quando você compra uma criptomoeda em uma *exchange*, você recebe um endereço de *wallet*, que na realidade é a uma chave pública de um sistema que usa criptografia assimétrica. A chave privada referente a esse endereço de *wallet* fica em poder da corretora (*exchange*). Assim, em uma corretora de criptomoedas você terá um endereço de *wallet* diferente para cada criptomoeda naquela corretora.

O endereço público de *wallet* você pode passar para qualquer pessoa que deseja lhe enviar Bitcoin, pois é um endereço público. Nenhum criminoso consegue furtar seus Bitcoins a partir do endereço público.

Contudo, se um criminoso virtual invadir o site da corretora onde você tem criptomoedas e tiver acesso às chaves privadas referentes aos seus endereços públicos de *wallet*, este criminoso poderá furtar todas as suas criptomoedas.

Isso mesmo! Sua segurança quando tem criptomoedas depende de manter seguras e confidenciais as chaves privadas de suas *wallets*.

Outra preocupação que você deve ter quando mantém criptomoedas no site de uma corretora (*exchange*) é com a segurança no acesso à sua conta. Se um criminoso virtual acessar sua conta no site da corretora como se fosse você, ele poderá transferir suas criptomoedas para as *wallets* dele em outro local. Assim, é essencial que você use uma senha forte de acesso

à sua conta no site da corretora e ative um segundo fator de autenticação (*two-factor authentication*).

- **Two-Factor Authentication (2FA):** Two-Factor Authentication (2FA) é um segundo fator de autenticação para acesso a contas de sites na web, ou seja, um fator de autenticação que vem depois de você digitar seu usuário e sua senha. Há vários tipos de 2FA, como a solicitação de um código enviado por SMS para o seu celular, um código enviado para seu e-mail ou um código gerado dinamicamente em um aplicativo de autenticação no seu celular, como o Google Authenticator e o Authy. O tipo de 2FA mais seguro e recomendado é o realizado por meio dos aplicativos Google Authenticator ou Authy.Basicamente, você instala um destes aplicativos no celular e, após fazer *login* na sua conta na *exchange*, na parte de configurações, você ativa o a verificação do Two-Factor Authentication (2FA). Ao ativar, aparecerá um *QR Code* que você terá que ler por meio da câmera do seu celular no Google Authenticator ou no Authy. Lido o *QR Code*, será gerado um código numérico que muda a cada 30 segundos. Toda vez que você acessar o site da exchange, após digitar o usuário e senha, aparecerá um campo solicitando o código gerado no Google Authenticator ou no Authy para esse site. Após digitar o código correto, você acessará sua conta.Perceba que se um criminoso virtual conseguir seu usuário e senha, ele não conseguirá acessar sua conta, pois será necessário um código gerado dinamicamente somente no seu celular. Há, porém, alguns riscos nesse processo. Se você perder o celular, por exemplo, perderá o acesso à sua conta. Por isso, quando ativou o Two-Factor Authentication (2FA), é importante ler o QR Code gerado em mais de um celular ou *tablet*, ou guardar em segurança o QR Code. Assim, se perder um celular, terá acesso por meio do outro, ou poderá ler o *QR Code* guardado em outro aparelho celular.

Oportunidades de investimento e de negócios no mercado de criptoativos

Entenda criptoativo como qualquer ativo digital que usa criptografia e *blockchain*, como criptomoedas, *tokens*, *stablecoins* etc. Normalmente convencionou-se chamar todas essas categorias de ativos digitais de criptomoedas ou criptoativos, o que é perfeitamente aceitável.

Há diversas oportunidades de investimento no mercado de criptoativos, sendo algumas delas listadas a seguir.

- **Criar criptomoeda** - criar uma criptomoeda ou *token* para angariar fundos para abrir um negócio;
- **Comprar criptomoeda no lançamento** - comprar uma criptomoeda ou *token* atrelada a um projeto de negócio na venda inicial (ICO ou IEO) e aguardar o negócio ser implementado e a moeda ganhar utilidade e valorizar;
- **Hold** - comprar criptomoedas já consolidadas e guardar na esperança de valorização futura;
- **Trade** - executar operações de trade com criptomoedas comprando quando os preços estão baixos e vendendo quando os preços sobem;
- **Arbitragem** - comprar criptomoedas em uma corretora (*exchange*) em que o preço está mais baixo e vender em outra em que o preço está mais alto;
- **Mineração ou *stake*** – participar do processo de validação de transações realizadas com uma criptomoeda e receber recompensa por isso.
- **Lending** – emprestar criptomoedas e receber rendimentos por isso.

Riscos do mercado de criptomoedas

A falta de regulamentação do mercado de criptomoedas têm atraído um grande número de golpistas criando pirâmides (esquema Ponzi) disfarçadas de empresas que operam com criptomoedas. Ofertas de lucros de 1%, 3% ou 10% ao dia não são incomuns na internet. Mesmo ofertas um pouco mais modestas, de 30% ao mês, já são indícios de golpes, pois nenhum investimento do mundo real tem condições de se manter pagando percentuais tão altos de lucros.

Atraídos pela ideia de lucro fácil e enriquecimento rápido trazida pelo *boom* no preço do Bitcoin na virada de 2017 para 218, que enriqueceu milhares de pessoas que compraram BTC no passado, muitas pessoas caem em propostas de golpistas oferecendo possibilidade de lucros irreais.

Além dos riscos associados a golpistas, há o risco natural da volatilidade de preços, que pode levar o preço das moedas a cair com o passar do tempo. Apesar de uma imensa comunidade de pessoas entusiastas do mercado de criptomoedas, na prática seu uso ainda tem sido muito discreto. Além disso, a tecnologia *blockchain* ainda não está suficiente madura para permitir um aumento da escalabilidade, podendo haver problemas se o aumento de usuários for exponencial. Assim, investir em criptomoedas é apostar em um mercado de incertezas, podendo levar a grandes lucros ou prejuízos equivalentes.

Considerando todos esses fatores de incerteza, muitos governos já começaram a adotar medidas de regulação do mercado de criptoativos. Há rumores de que a China está criando sua própria criptomoeda. Outros países podem seguir o mesmo caminho. Alguns governos adotaram postura de proibição e penalização pelo uso desses ativos digitais.

As criptomoedas foram criadas em uma filosofia de liberdade em relação ao Estado centralizador. A regulação pode afastar as pessoas que buscam essa liberdade de negociação. Porém, por outro lado, regulamentar pode facilitar a aplicação dos rigores da lei aos golpistas e atrair pessoas que veem no Estado um agente digno de confiança.

Mas será que, se os governos criarem suas próprias criptomoedas oficiais, haverá espaço para as diversas criptomoedas não oficiais existentes hoje?

São muitas questões e muitas incertezas que devem nos guiar para medir o nível de risco que estamos dispostos a correr quando entramos nesse mercado.

REFERÊNCIAS BIBLIOGRÁFICAS

BINANCE. **O que é Ethereum?**. 2019. Disponível em <*https://www.binance.vision/pt/blockchain/what-is-ethereum*>. Acesso em: 4 out. 2019.

BINANCE. **O que são Contratos Inteligentes?**. 2019. Disponível em: <*https://www.binance.vision/pt/blockchain/what-are-smart-contracts*>. Acesso em: 3 set. 2019.

BINANCE. **Proof of Stake**. 2019. Disponível em: <*https://www.binance.vision/pt/blockchain/proof-of-stake-explained*>. Acesso em: 3 set. 2019.

CERT.BR. **Criptografia de chave simétrica e de chaves assimétricas.** 2012. Disponível em <*https://cartilha.cert.br/criptografia/*>. Acesso em: 2 set. 2019.

GALEON, D. **Mining Bitcoin costs more energy than what 159 countries consume in a year**. 2017. Disponível em: <*https://futurism.com/mining-bitcoin-costs-more-energy-159-countries-consume-year*>. Acesso em: 4 set. 2019.